WHAT IS CLAIMED IS:

1. A scalable on-line system for printing value bearing items (VBI) comprising:

a client system for interfacing with one or more users; and

a scalable server system capable of communicating with the client system over a communication network comprising:

a database remote from the users including information about the users;

a stateless cryptographic module for authenticating the one or more users; and

a plurality of security device transaction data stored in the database for ensuring authenticity of the one or more users, wherein each security device transaction data can be processed in the server system in a stateless manner.

2. The system of claim 1, wherein each security device transaction data is related to a user.

3. The system of claim 2, wherein the security device transaction data related to a user is loaded into the cryptographic module when the user requests to operate on a value bearing item.

4. The system of claim 3, wherein the security device transaction data related to a user is updated and returned to the database.

5. The system of claim 1, further comprising at least one more stateless cryptographic module, wherein each cryptographic module is capable of processing any of the plurality of security device transaction data.

6. The system of claim 5, wherein a user can be authenticated using any of the cryptographic modules.

7. The system of claim 5, further comprising computer executable code for load-balancing to route user requests to the at least one more cryptographic module.

8. The system of claim 5, further comprising computer executable code for load-balancing to distribute traffic among the multiple cryptographic modules.

9. The system of claim 1, wherein the cryptographic module is capable of authenticating any of the one or more users.

10. The system of claim 1, wherein the database is partitioned across a plurality of physical databases.

11. The system of claim 1, wherein the cryptographic module performs cryptographic function on a transaction related to the database.

12. The system of claim 1, further comprising computer executable code for password authentication to prevent unauthorized access to the database.

13. The system of claim 1, wherein the database stores a first set of one or more last database transactions and the cryptographic module stores a second set of one or more last database transactions for comparison with the first set of one or more last database transactions stored in the database to verify each database transaction.

14. The system of claim 13, wherein the cryptographic module prevents further database transactions if the second set of one or more last transaction stored in the cryptographic module does not compare with the first set of one or more last transaction stored in the database.

15. The system of claim 1, wherein the cryptographic module includes a data validation subsystem for allowing the module to verify that data is up to date and an auto-recovery subsystem for automatically re-synchronize the module with the data.

16. The system of claim 1, wherein the cryptographic module includes a computer executable code for preventing unauthorized modification of data.

17. The system of claim 1, wherein the cryptographic module includes a computer executable code for ensuring the proper operation of cryptographic security and VBI related meter functions.

18. The system of claim 1, wherein the cryptographic module includes a computer executable code for supporting multiple concurrent users.

19. The system of claim 1, wherein the database includes one or more indicium data elements, data for account maintenance, and data for revenue protection.

20. The system of claim 1, wherein the database includes virtual meter information.

21. The system of claim 1, wherein the database includes descending register data.

22. The system of claim 1, wherein the value bearing item is a mail piece.

23. The system of claim 22, wherein the postal indicium comprises a digital signature.

24. The system of claim 1, wherein the cryptographic module performs cryptographic function on validation information according to a user request for printing a VBI.

25. The system of claim 1, wherein the cryptographic module generates data sufficient to print a postal indicium in compliance with postal service regulation on a mail piece.

26. The system of claim 1, wherein the value bearing item is a ticket.

27. The system of claim 1, wherein a bar code is printed on the value bearing item.

28. The system of claim 1, wherein the value bearing item is a coupon.

29. The system of claim 1, wherein the value bearing item is currency.

30. The system of claim 1, wherein the value bearing item is a voucher.

31. The system of claim 1, wherein the value bearing item is a traveler's check.

32. The system of claim 1, wherein each security device transaction data includes one or more of an ascending register value, a descending register value, a respective cryptographic module ID, an indicium key certificate serial number, a licensing ZIP code, a key token for an indicium signing key, user secrets, a key for encrypting user secrets, date and time of last transaction, last challenge received from a respective client subsystem, an operational state of the respective module, expiration dates for keys, and a passphrase repetition list.

33. The system of claim 1, wherein each security device transaction data includes one or more of a private key, a public key, and a public key certificate, wherein the private key is used to sign module status responses and a VBI which, in conjunction with a public key certificate, demonstrates that the module and the VBI are authentic.

34. The system of claim 1, wherein the cryptographic module is capable of performing one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms.

35. The system of claim 1, wherein the server system further comprises one or more of a postal server subsystem, a provider server subsystem, an e-commerce subsystem, a staging subsystem, a client support subsystem, a decision support subsystem, a SMTP subsystem, an address matching service subsystem, a SSL proxy server subsystem, and a web server subsystem.

36. The system of claim 1, wherein the database includes one or more of a postal database, a provider database, an e-commerce database, and a membership database.

37. The system of claim 1, further comprising an address matching server for verifying a correct address specified by a user.

38. The system of claim 1, further comprising a printer driver database for storing supported printer driver information.

39. A method for printing value-bearing items (VBI) via a communication network including a client system, and a scalable server system, the method comprising the steps of:

interfacing with one or more users via the client system;

communicating with the client system over the communication network;

storing user information in a database accessible through the network;

authenticating the one or more users using a scalable cryptographic module; and

storing in the database a plurality of security device transaction data for ensuring authenticity of the one or more users, wherein each security device transaction data can be processed in the server system in a stateless manner.

40. The method of claim 39, wherein each security device transaction data is related to a user.

41. The method of claim 40, further comprising the step of loading the security device transaction data related to a user into the cryptographic module when the user requests to operate on a value bearing item.

42. The method of claim 41, further comprising the steps of updating and returning the security device transaction data related to a user to the database.

43. The method of claim 39, further comprising the step of adding at least one more stateless cryptographic module, wherein each cryptographic module is capable of processing any of the plurality of security device transaction data.

44. The method of claim 39, further comprising the step of authenticating a user using any of the cryptographic modules.

45. The method of claim 43, further comprising the step of load-balancing to route user requests to the at least one more cryptographic module.

46. The method of claim 43, further comprising the step of load-balancing to distribute traffic among the multiple cryptographic modules.

47. The method of claim 39, further comprising the step of the authenticating any of the one or more users using the cryptographic module.

48. The system of claim 1,further comprising the step of partitioning the database across a plurality of physical databases.

49. The method of claim 39, further comprising the step of encrypting database transactions using the cryptographic module.

50. The method of claim 39, further comprising the steps of verifying a user password before granting access to the database.

51. The method of claim 39, further comprising the steps of

storing one or more last database transactions in the database;

storing one or more last database transactions in the cryptographic module; and

comparing the one or more last database transactions stored in the database with the one or more last database transactions stored in the cryptographic module to verify each database transaction.

52. The method of claim 39, further comprising the step of encrypting transactions related to the database using the cryptographic module.

53. The method of claim 39, further comprising the steps of storing one or more last database transactions in the database, storing one or more last database transactions in the cryptographic module for comparison with the one or more last database transactions stored in the database to verify each database transaction.

54. The method of claim 53, further comprising the step of preventing further database transactions if the one or more last transaction stored in the cryptographic module does not compare with the one or more last transaction stored in the database.

55. The method of claim 39, further comprising the steps of preventing unauthorized modification of data using the cryptographic module.

56. The method of claim 39, further comprising the steps of verifying that the database is up to date.

57. The method of claim 39, further comprising the steps of automatically re-synchronizing the cryptographic module with the database.

58. The method of claim 39, further comprising the step of ensuring the proper operation of cryptographic security and VBI related meter functions.

59. The method of claim 39, further comprising the steps of supporting multiple concurrent operators.

60. The method of claim 39, further comprising the steps of:

storing information about a number of last transactions in a respective internal register of each of the one or more cryptographic devices;

storing a table including the information about a last transaction in the database;

comparing the information saved in the respective device with the respective information saved in the database; and

loading a new transaction data if the respective information stored in the device compares with the respective information stored in the database.

61. The method of claim 39, further comprising the step of storing data for creating one or more indicium, account maintenance, and revenue protection.

62. The method of claim 39, further comprising the step of printing a mail piece.

63. The method of claim 62, wherein the mail piece includes a digital signature.

64. The method of claim 62, wherein the mail piece includes a postage amount.

65. The method of claim 62, wherein the mail piece includes an ascending register of used postage and descending register of available postage.

66. The method of claim 50, further comprising the step of printing a ticket.

67. The method of claim 39, further comprising the step of printing a bar code.

68. The method of claim 39, further comprising the step of printing a coupon.

69. The method of claim 39, further comprising the step of printing currency.

70. The method of claim 39, further comprising the step of printing a voucher.

71. The method of claim 39, further comprising the step of printing a traveler's check.

72. The method of claim 39, wherein the security device transaction data includes an ascending register value, a descending register value, a respective cryptographic device ID, an indicium key certificate serial number, a licensing ZIP code, a key token for an indicium signing key, user secrets, a key for encrypting user secrets, date and time of last transaction, last challenge received from a respective client subsystem, an

operational state of the respective device, expiration dates for keys, and a passphrase repetition list.

73. The method of claim 39, further comprising the step of performing one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms using each of the cryptographic devices.

74. The method of claim 39, further comprising the step keeping track of user accesses to a vendor website using a website database.

75. The method of claim 39, further comprising the step of storing postal transaction data, financial transaction data, customer marketing information, commerce product information, meter license information, meter resets, meter history, and meter movement information in an offline database.

76. The method of claim 39, further comprising the step of storing customer information, financial transactions, and information for marketing queries in a data warehouse database.

77. The method of claim 39, further comprising the steps of authorizing and capturing funds from a customer's account and transferring the funds to a vendor's account using an e-commerce server.

78. The method of claim 39, further comprising the step of verifying a correct address specified using a user using an address matching server.

79. The method of claim 39, further comprising the step of storing supported printer driver information in a printer driver database.